UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

CHANDRA TATE, on behalf of herself and all others similarly situated, Plaintiff, v. **EYEMED VISION CARE, LLC,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Chandra Tate ("Plaintiff"), by and through her attorneys, upon personal knowledge as to herself and her own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Class Action Complaint ("Complaint") against Defendant EyeMed Vision Care, LLC ("Defendant" or "EyeMed"), individually and on behalf of all others similarly situated based on Defendant's failure to properly safeguard its customers' personally identifiable information ("PII"), including current and former customer's full names, residential addresses, dates of birth, phone numbers, email addresses, vision insurance account identification numbers, health insurance account identification numbers, Medicaid and Medicare numbers, Social Security numbers, birth or marriage certificates, and driver's license, passport or other government identification numbers and information. Defendant also failed to properly safeguard its customers' protected health information ("PHI") exposed in the breach, including medical diagnoses and medical treatment information.

2. EyeMed is one of the largest and fastest growing vision benefits companies in the United States. It has over 60 million funded benefit members through a nationwide network of providers that includes optometrists, ophthalmologists, opticians, and retailers. EyeMed offers several different plans, all of which provide various levels of discounts on exams and vision products such as eyeglass frames and lenses, contact lenses, and other eye care services. The company serves a customer base that includes large corporations, government entities, and health insurers, including but not limited to Aetna, Blue Cross Blue Shield of Tennessee and Nippon Life Benefits.

3. On June 24, 2020, as a result of EyeMed's lax security and monitoring protocols, criminals gained unauthorized access to an EyeMed email inbox. For seven days, these criminals maintained unfettered access to the breached email account. During this time, the email account was used to send phishing emails to EyeMed's customers. The breach of the email account also allowed the criminals to obtain the sensitive PII and PHI of EyeMed's customers stored in the account.

4. It was not until July 1, 2020 that EyeMed discovered the breach and took steps to block unauthorized access to the account. By that time, the PII and PHI of its customers had already fallen into the hands of the ill-intentioned criminals that accessed the account.

5. Defying all bounds of reasonableness, despite learning of the breach on or about July 1, 2020, EyeMed did not notify customers affected by the breach until December of 2020. And it did not prioritize the victims of the breach; instead, months before it started notifying customers, EyeMed notified its industry partners such as Aetna. There is simply no excuse for taking so long to notify customers, and for de-prioritizing the actual victims of its lax security and safeguards.

6. EyeMed did not adequately safeguard Plaintiff's data, and now she and apparently millions of other patients are the victims of a significant data breach that will negatively affect them for years.

7. EyeMed is responsible for allowing this data breach through its failure to implement and maintain reasonable safeguards and failure to comply with industry-standard data security practices.

8. Despite its role in managing so much sensitive and personal information, during the duration of the data breach, EyeMed failed to recognize and detect unauthorized third parties accessing its email system, and failed to recognize the substantial amounts of data that had been compromised. This was, in part, because of, but also part and parcel with, EyeMed's failure to take the appropriate steps to investigate the numerous red flags, each of which individually should have told EyeMed that its systems were not secure.

9. EyeMed had numerous statutory, regulatory, contractual, and common law obligations, including those based on its affirmative representations to Plaintiff and class members, to keep their PII, including PHI, confidential, safe, secure, and protected from unauthorized disclosure or access.

10. Plaintiff and those similarly situated rely upon EyeMed to maintain the security and privacy of the PII and PHI entrusted to it; when providing their PII and or PHI, they reasonably expected and understood that EyeMed would comply with its obligations to keep the information secure and safe from unauthorized access.

11. In this day and age of regular and consistent data security attacks and data breaches, in particular in the healthcare industry and retail services, EyeMed's data security breach is particularly egregious.

12. As a result of EyeMed's failures, Plaintiff and the class members are at a significant risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come. Just as their PII and PHI was stolen because of its inherent value in the black market, now the inherent value of Plaintiff's and the class members' PII and PHI in the legitimate market is significantly and materially decreased. To make matters worse, the injuries described were exacerbated by EyeMed's failure to timely inform and notify Plaintiff and the class members of the data breach and their injuries. Furthermore, by failing to provide adequate notice, EyeMed intentionally prevented Plaintiff and prospective class members from protecting themselves from the potential damages arising out of the data breach.

13. On information and belief, as a result of this massive data breach, millions of EyeMed's customers have suffered exposure of PII and PHI entrusted to EyeMed.

14. In addition, based on Defendant's actions, Plaintiff and the proposed class have received services that were and are inferior to those for which they have contracted, and have not been provided the protection and security Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII and PHI.

15. Plaintiff and members of the proposed class have suffered actual and imminent injuries as a direct result of the data breach. The injuries suffered by Plaintiff and the proposed class as a direct result of the data breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the consequences of the data breach and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach; (d) the imminent injury arising from potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or

criminals; (e) damages to and diminution in value of their personal data entrusted to EyeMed and with the mutual understanding that EyeMed would safeguard Plaintiff's and class members' personal data against theft and not allow access and misuse of their personal data by others; (f) the reasonable value of the PII entrusted to EyeMed; and (g) the continued risk to their personal data, which remains in the possession of EyeMed and which is subject to further breaches so long as EyeMed fails to undertake appropriate and adequate measures to protect Plaintiff's and class members' personal data in its possession.

16. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the data breach.

17. Accordingly, Plaintiff, on behalf of herself and other members of the class, asserts claims for breach of implied contract, negligence, bailment, and unjust enrichment, and seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Chandra Tate

18. Plaintiff Chandra Tate[1] is a natural person and a resident of South Carolina. From 2016 through 2019, she and her family used EyeMed for their vision care benefits. This included submitting claims to EyeMed for the purchase of prescription lenses from Walmart and Sam's Club.

19. Plaintiff entrusted her PII, PHI, and other confidential information such as contact

[1] Plaintiff's name was previously Chandra Price. However, she married in February of 2020 and assumed the surname of Tate.

information, health insurance policy information, prescription information, medical conditions, and Social Security number to EyeMed with the reasonable expectation and understanding that EyeMed would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used EyeMed's services had she known that EyeMed would not take reasonable steps to safeguard her sensitive PII and PHI.

20. In mid-December of 2020, more than five months after EyeMed learned of the data breach, Plaintiff received a letter from EyeMed, dated December 7, 2020, notifying her that she had been identified as an individual impacted by the data breach that occurred from June 24, 2020 through July 1, 2020. A copy of the letter is attached hereto as **Exhibit A**. Before receiving this letter, Plaintiff was unaware that any breach had occurred or that her PII and PHI had been compromised.

21. Since learning about the breach, Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the breach of her sensitive personal, financial, and health information, as well as the breach of her daughter's sensitive personal, financial, and health information (which was also compromised in the breach). As a result of the breach and anxiety it has caused, she estimates that she reviews her credit information and statements twice a week, and she reviews her bank accounts nearly every day. Before the breach, she typically only reviewed her credit information once or twice a month, and only reviewed her bank accounts once a month. Furthermore, following the breach, she has received scam and phishing phone calls nearly every day. For example, towards the end of November 2020, Plaintiff received calls from scammers purporting to work for the Internal Revenue Service and Social Security Administration.

22. Plaintiff and her family have used the paid monitoring service LifeLock for roughly the past year and a half. Following the breach, she received a notification from LifeLock informing her that it had identified suspicious activity on her accounts. Plaintiff had intended to discontinue the LifeLock service in an attempt to reduce her monthly bills. However, as a result of the EyeMed data breach, Plaintiff has continued to use and pay for the LifeLock service for her and her family. This service costs her roughly $65 per month.

23. Around the time of the data breach, an unknown individual used Plaintiff's financial information without her permission to open an account with Amazon Prime. Plaintiff was charged for these services despite not having an Amazon Prime account until she noticed the charges in August of 2020. As a result, Plaintiff was also forced to close the bank account linked to the Amazon Prime charges and open a new bank account.

24. Plaintiff's injuries will be redressed by a favorable outcome in this litigation because she seeks compensatory damages.

Defendant EyeMed Vision Care, LLC

25. EyeMed is a Delaware limited liability company with its principal place of business in Mason, Ohio. It is a wholly owned subsidiary of Luxottica of America, Inc., which is similarly headquartered in Mason, Ohio.

26. EyeMed requires its customers to provide contact information (such as name, email, and shipping address), and financial information (such as Health Services Account or other credit card account information). As part and parcel of providing and/or accepting insurance, customers must also provide their sensitive health information and other personal information (such as dates of birth and Social Security numbers, that EyeMed requests).

27. EyeMed also creates electronic health records of its customers by gathering medical

information from them. This information comes from the customers and from other individuals or organizations, such as referring physicians, other doctors, and/or insurance plans.

28. EyeMed provides that each of its affiliates are permitted to share customer PII and other information across brands.

JURISDICTION & VENUE

29. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Plaintiff (and many members of the class) and Defendant are citizens of different states.

30. This Court has general personal jurisdiction over EyeMed because EyeMed's principal place of business is in Mason, Ohio.

31. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and EyeMed conducts substantial business in this District.

FACTUAL ALLEGATIONS

32. EyeMed is one of the largest vision benefits companies in the United States, providing vision benefits to over 60 million members.[2] As of 2014, it is the second largest vision benefits companies in the United States.[3]

33. As with all benefit or insurance companies, upon information and belief, use of EyeMed's services requires disclosure of PII and PHI to EyeMed by all of its over 60 million members.

[2] https://eyemed.com/en-us/about-us, last accessed 1/12/2021.
[3] https://en.wikipedia.org/wiki/Luxottica, last accessed 1/12/2021.

34. EyeMed is fully aware of how sensitive the PII and PHI it stores and maintains is. It is also aware of how much PII and PHI it collects, uses, and maintains from each Plaintiff or class member. EyeMed offers services related to healthcare treatment and the provision of insurance.

35. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiff's and the class members' PII and PHI, EyeMed assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII and PHI it collected and stored.

EyeMed knew that it was and continues to be a prime target for cyberattacks.

36. EyeMed knew that it was an ideal target for hackers and those with nefarious purposes related to consumers data. It processed and saved multiple types and many levels of PII and PHI through its many types of businesses.

37. Realizing that its data is a target of hackers, EyeMed's Privacy Policy[4] states:

> The security of your personal information is important to us. We follow generally accepted industry standards to protect the personal information submitted to us, and to guard that information against loss, misuse or alteration. When you enter personal information on our Site, we encrypt transmissions involving such information using secure protocols.

38. Yet, EyeMed did not follow generally accepted industry standards to protect its customers' sensitive PII and PHI.

39. EyeMed processed employer and payment information, in addition to all the information about vision, vision healthcare, and any other information that it might demand as a benefits provider, such as Social Security number, age, gender, and prior health history.

[4] https://eyemed.com/en-us/online-privacy-policy, last accessed 1/12/2021.

40. The seriousness with which EyeMed should have taken its data security is shown by the number of data breaches perpetrated in the healthcare and retail industries in the last few years.

41. Despite knowledge of the prevalence of healthcare and retail data breaches, EyeMed failed to prioritize its customers' data security by implementing reasonable data security measures to detect and prevent unauthorized access to the tens of millions of sensitive data points of its customers. As a highly successful insurance benefits company, EyeMed had the resources to invest in the necessary data security and protection measures. Yet, it did not.

42. EyeMed failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures presented to customers in December of 2020 but which occurred in June of 2020.

43. Despite its awareness, EyeMed did not take the necessary and required minimal steps to secure Plaintiff's and the class members' PII and PHI. As a result, hackers breached and stole important PII and PHI from likely millions of EyeMed customers in late June 2020.

EyeMed Failed to Timely Notify Victims of the Breach

44. On July 1, 2020, EyeMed became aware that a breach occurred. It did not notify the victims of the breach at that time or for months later. Rather, it first notified large corporations that it partners with or performed services for. For example, almost three months after it learned of the breach, on September 28, 2020, EyeMed informed the insurance company Aetna of the breach, which had exposed the PII and PHI of approximately 484,157 Aetna customers alone.[5]

45. Inexplicably, it was not until almost six months after the breach (mid-December

[5] https://www.healthcareitnews.com/news/nearly-500k-aetna-members-affected-eyemed-security-inciden, last accessed 1/12/2021.

2020) that EyeMed took the necessary step of informing individuals such as Plaintiff and members of the class via letter that it "discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book." For example, Plaintiff received the following in a letter (attached as **Exhibit A**) received in mid-December 2020 and dated December 7, 2020:

> On July 1, 2020, EyeMed discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book….It was determined that the unauthorized individual first gained access to the mailbox on June 24, 2020, and that access terminated on July 1, 2020.
> …
> The mailbox contained information about individuals who formerly or currently receive vision benefits through EyeMed.
> …
> Following a detailed analysis and review of all potentially compromised emails and files, EyeMed identified the names of all individuals who were impacted, as well as the type of information included in those files. Personal information that may have been accessed could include the following types of information: full name, address, date of birth, phone number, email address, and vision insurance account/identification number.

46. EyeMed's letter to Plaintiff and members of the class was patently deficient because it failed to disclose the full range of information that was compromised in the breach. For example, EyeMed's website discloses information that was exposed in the breach but not mentioned in its letters to Plaintiff and members of the class, including: health insurance account/identification numbers, Medicaid or Medicare numbers, driver's license or other government identification numbers, birth or marriage certificates, Social Security numbers, financial information, medical diagnoses and conditions, treatment information, and/or passport numbers.[6]

47. EyeMed's disclosure letter also described what it was doing to remedy its flawed

[6] *See* https://eyemed.com/en-us/notice, last accessed 1/12/2021.

security protocols:

> EyeMed is committed to safeguarding your personal information and has taken immediate steps to enhance the protections that were already in place before this incident. In addition to the investigation, EyeMed made changes to how authorized individuals access the EyeMed network and required immediate complex password changes to all our employee accounts. EyeMed is also reinforcing and providing additional mandatory security awareness training.

48. EyeMed "encourage[d]" Plaintiff and the class members "to remain vigilant," and told them that if they see suspicious or unusual activity on their accounts, **not to tell EyeMed**, but to report it to someone else.

49. Despite knowing since July 1, 2020 that there had been a data breach, EyeMed did not issue notice to those affected within the timeframe required by law or its own Privacy Policy.

50. For example, in its HIPAA Notice of Privacy Practices, EyeMed states:

> If we discover that your health information has been breached (for example, disclosed to or acquired by an unauthorized person, stolen, lost, or otherwise used or disclosed in violation of applicable privacy law) and the privacy or security of the information has been compromised, we must notify you of the breach without unreasonable delay and in *no event later than 60 days following our discovery of the breach*.[7]

EyeMed Owed a Duty to Plaintiff and Class Members to Adequately Safeguard Their PII and to Provide Timely Notice of the Breach of its Systems

51. EyeMed is well aware of the importance of security in maintaining personal information (particularly health and medical information), and the value its users place on keeping their PII and PHI secure.

52. EyeMed owes a duty to Plaintiff and the class members to maintain adequate

---

[7] https://eyemed.com/en-us/hipaa-notice-of-privacy-practices, last accessed 1/12/2020 (emphasis added).

security and to protect the confidentiality of their personal data.

53. EyeMed owes a further duty to its current and former users to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

The Sort of PII at Issue Here is Particularly Valuable to Hackers

54. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

55. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

56. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get

credit.[8]

57. Here, the unauthorized access by the hackers left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and class members stolen in the EyeMed security breach constitutes a dream for hackers and a nightmare for Plaintiff and the class. Plaintiff's and class members' stolen personal data represents essentially one-stop shopping for identity thieves.

58. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[9] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[10]

59. More recently the FTC has released its updated publication on protecting PII for businesses, which include instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

60. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect customers' PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC

---

[8] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 13, 2020).

[9] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Nov. 13, 2020).

[10] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

Act, 15 U.S.C. § 45.

61. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

62. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other PII on a number of Internet websites. Plaintiff's and class members' personal data that was stolen has a high value on both legitimate and black markets.

63. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[12]

64. Consumers rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable.

65. Notably, one study on website privacy determined that U.S. consumers valued the

---

[11] *See* http://www.gao.gov/new.items/d07737.pdf at 29 (last visited Nov. 13, 2020).

[12] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited Nov. 13, 2020).

restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[13] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

66. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent refund. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

67. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[14] Former and current users of EyeMed systems whose Social Security numbers have been compromised will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

---

[13] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 14, 2021).

[14] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

68. Again, because the information EyeMed allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiff and the class will continue to grow, and Plaintiff and the class will continue to be at substantial risk for further imminent and future harm.

EyeMed's Post-Breach Activity was Inadequate

69. Personal, health, and financial information can be sold on the black-market almost immediately. As Illinois Attorney General Lisa Madigan aptly put it, "the second somebody gets your credit or debit card information, it can be a matter of hours or days until it's sold on the black market and someone's starting to make unauthorized transactions."[15] Thus, the compromised information could be used weeks or even months before the receipt of any letter from EyeMed and EyeMed's proposed solutions to the potential fraud are, therefore, woefully deficient.

70. Immediate notice of a security breach is essential to protect people such as Plaintiff and the class members. EyeMed failed to provide such immediate notice, in fact taking at least five to six months to disclose to individual customers that there had been a breach, thus further exacerbating the damages sustained by Plaintiff and the class resulting from the breach.

71. Such failure to protect Plaintiff's and the class members' PII and PHI, and timely notify of the breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because many of the data points stolen are persistent—for example, Social Security number, name, address, email address, and medical history—as opposed to transitory—for example, the date of an appointment, criminals who purchase the PII and PHI belonging to Plaintiff and the class members do not need to use the

[15] Phil Rosenthal, *Just assume your credit and debit card data were hacked*, http://www.chicagotribune.com/business/columnists/ct-data-breach-credit-scam-rosenthal-1001-biz-20140930-column.html#page=1 (last visited Jan. 14, 2021).

information to commit fraud immediately. The PII and PHI can be used or sold for use years later.

72. A single person's PHI can fetch up to $350 on the dark web. This is due, in part, to the broad scope and comprehensive nature of the data and information, which can be used to steal identities for illegal drug or medical purchases or defraud insurers. Allowing hackers to steal this type of information is particularly nefarious, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before healthcare-related fraud is spotted.

73. Every year, victims of identity theft lose billions of dollars. And reimbursement is only the beginning, as these victims usually spend hours and hours attempting to repair the impact to their credit, at a minimum.

74. Plaintiff and the class members are at constant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of the EyeMed's actions and the data breach. They have suffered real and tangible loss, including but not limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case, but hitherto kept deliberately hidden by EyeMed.

CLASS ACTION ALLEGATIONS

75. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3) are met with respect to the class defined below.

76. Under Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action

as a national class action for themselves and all members of the following class of similarly situated persons:

The Nationwide Class

> All persons who reside in the United States whose personal data was compromised as a result of the security breach discovered by EyeMed on or about July 1, 2020.

77. Excluded from the class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

78. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating subclasses, as necessary.

79. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

80. All members of the proposed class are readily ascertainable in that EyeMed has access to addresses and other contact information for all members of the class, which can be used for providing notice to class members.

81. ***Numerosity***. The class is so numerous that joinder of all members is impracticable. The class includes millions of individuals whose personal data was compromised by the EyeMed security breach.

82. ***Commonality***. There are numerous questions of law and fact common to Plaintiff and the class, including the following:

- whether EyeMed engaged in the wrongful conduct alleged in this Complaint;

- whether EyeMed's conduct was unlawful;
- whether EyeMed failed to implement and maintain reasonable systems and security procedures and practices to protect customers' personal data;
- whether EyeMed unreasonably delayed in notifying affected customers of the security breach;
- whether EyeMed owed a duty to Plaintiff and members of the class to adequately protect their personal data and to provide timely and accurate notice of the EyeMed security breach to Plaintiff and members of the class;
- whether EyeMed breached its duties to protect the personal data of Plaintiff and members of the class by failing to provide adequate data security and failing to provide timely and adequate notice of the EyeMed security breach to Plaintiff and the class;
- whether EyeMed's conduct was negligent;
- whether EyeMed knew or should have known that its computer systems were vulnerable to attack;
- whether EyeMed's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of class members' personal data;
- whether EyeMed wrongfully or unlawfully failed to inform Plaintiff and members of the class that it did not maintain computers and security practices adequate to reasonably safeguard customers' financial and personal data;
- whether EyeMed should have notified the public, Plaintiff, and class members immediately after it learned of the security breach;
- whether Plaintiff and members of the class suffered injury, including ascertainable losses, as a result of EyeMed's conduct (or failure to act);
- whether EyeMed breached its duties to Plaintiff and the class as a bailee of PII and PHI entrusted to it and for which EyeMed owed a duty to safeguard and of safekeeping;
- whether Plaintiff and members of the class are entitled to recover damages; and
- whether Plaintiff and class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

83. ***Typicality***. Plaintiff's claims are typical of the claims of the class in that Plaintiff, like all class members, had their personal data compromised, breached and stolen in the EyeMed security breach. Plaintiff and all class members were injured through the uniform misconduct of

EyeMed described in this Complaint and assert the same claims for relief.

84. ***Adequacy***. Plaintiff and counsel will fairly and adequately protect the interests of the class. Plaintiff has retained counsel who are experienced in class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other members of the class.

85. ***Predominance***. The questions of law and fact common to class members predominate over any questions which may affect only individual members.

86. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, EyeMed's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the class. Plaintiff and class members have been harmed by EyeMed's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to EyeMed's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

87. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

88. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual class members would create a risk of inconsistent

or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for EyeMed. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each class member.

COUNT I — NEGLIGENCE

89. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

90. EyeMed owed a duty to Plaintiff and members of the class to safeguard the sensitive PII and PHI that they were required to provide EyeMed as a condition of receiving EyeMed's services. EyeMed was required to prevent foreseeable harm to Plaintiff and the class members, and therefore had a duty to take reasonable steps to safeguard sensitive PII and PHI from unauthorized release or theft.

91. In other words, EyeMed was required to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal, health, and financial information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing EyeMed's security systems to ensure that Plaintiff's and class members' personal, health, and financial information in EyeMed's possession was adequately secured and protected.

92. EyeMed further owed a duty to Plaintiff and class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

93. There is a very close connection between EyeMed's failure to follow reasonable security standards to protect its current and former users' personal data and the injury to Plaintiff

and the class. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

94. If EyeMed had taken reasonable security measures, data thieves would not have been able to take the personal information of millions of current and former users of EyeMed's services. The policy of preventing future harm weighs in favor of finding a special relationship between EyeMed and Plaintiff and the class. If companies are not held accountable for failing to take reasonable security measures to protect their customers' personal data, they will not take the steps that are necessary to protect against future security breaches.

95. EyeMed owed a duty to timely disclose the material fact that EyeMed's computer systems and data security practices were inadequate to safeguard users' personal, health, and financial data from theft.

96. EyeMed breached these duties by the conduct alleged in the Complaint by, including without limitation, failing to protect its customers' personal, health, and financial, information; failing to maintain adequate computer systems and data security practices to safeguard customers' personal, health, and financial information; failing to disclose the material fact that EyeMed's computer systems and data security practices were inadequate to safeguard customers' personal, health, and financial data from theft; and failing to disclose in a timely and accurate manner to Plaintiff and members of the class the material fact of the data breach.

97. As a direct and proximate result of EyeMed's failure to exercise reasonable care and use commercially reasonable security measures, the personal data of current and former EyeMed users was accessed by ill-intentioned criminals who could and will use the information

to commit identity or financial fraud. Plaintiff and the class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their personal data.

98. As a proximate result of this conduct, Plaintiff and the other class members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiff and the class have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts to protect their PII and prevent the unauthorized use of their PII.

COUNT II — BAILMENT

99. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

100. Plaintiff and the class delivered their personal, health, and financial information to EyeMed for the exclusive purpose of obtaining services.

101. The PII and PHI is intangible personal property belonging to Plaintiff and the class members.

102. In delivering their personal data to EyeMed, Plaintiff and class members intended and understood that EyeMed would adequately safeguard their personal data.

103. EyeMed accepted possession of Plaintiff's and class members' personal data for the purpose of providing work-related services to Plaintiff and class members.

104. A bailment (or deposit) was established for the mutual benefit of the parties. By accepting possession of Plaintiff's and class members' personal data, EyeMed understood that Plaintiff and class members expected EyeMed to adequately safeguard their personal data. Furthermore, EyeMed understood that it had ongoing responsibilities to account for the information provided by its customers.

105. For example, under its Notice of Privacy Practices,[16] EyeMed warranted that it would notify customers if their personal information was exposed no later than 60 days following discovery of the breach. Additionally, upon request, EyeMed was required to provide customers with "a list of instances in which we or our business associates disclosed your health information," as well as provide access to customers upon request to review or receive copies of the health information that EyeMed stored.[17]

106. During the bailment (or deposit), EyeMed owed a duty to Plaintiff and class members to exercise reasonable care, diligence, and prudence in protecting their personal data as well as a duty to safeguard personal information properly and maintain reasonable security procedures and practices to protect such information. Defendant breached this duty.

107. EyeMed breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and class members' personal, health, and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and class members' personal, health, and financial information. Defendant also breached its duty to account for the information it stored on behalf of Plaintiff and the class members and to notify them no later than 60 days after learning of a data breach.

108. As a proximate result of this conduct, Plaintiff and the other class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III — BREACH OF IMPLIED CONTRACT

109. Plaintiff incorporates by all other allegations in the Complaint as if fully set forth here.

[16] https://eyemed.com/en-us/hipaa-notice-of-privacy-practices, last accessed 1/12/2021.
[17] *Id.*

110. Plaintiff and the class delivered their personal, health, and financial information to EyeMed as part of the process of obtaining services provided by EyeMed.

111. Plaintiff and members of the class entered into implied contracts with EyeMed under which EyeMed agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and class members that their data had been breached and compromised.

112. In providing such data, Plaintiff and the other members of the class entered into an implied contract with EyeMed whereby EyeMed became obligated to reasonably safeguard Plaintiff's and the other class members' sensitive, non-public information.

113. In delivering their personal data to EyeMed, Plaintiff and class members intended and understood that EyeMed would adequately safeguard their personal data.

114. Plaintiff and the class members would not have entrusted their private and confidential financial, health, and personal information to Defendants in the absence of such an implied contract.

115. EyeMed accepted possession of Plaintiff's and class members' personal data for the purpose of providing services to Plaintiff and class members.

116. Had EyeMed disclosed to Plaintiff and members of the class that EyeMed did not have adequate computer systems and security practices to secure users' and former users' personal data, Plaintiff and members of the class would not have provided their PII and PHI to EyeMed.

117. EyeMed recognized that its users' and former users' personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and members of the class.

118. Plaintiff and members of the class fully performed their obligations under the implied contracts with EyeMed.

119. EyeMed breached the implied contract with Plaintiff and the other members of the class by failing to take reasonable measures to safeguard their data.

120. As a proximate result of this conduct, Plaintiff and the other class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV — UNJUST ENRICHMENT

121. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

122. Plaintiff and class members conferred a monetary benefit on EyeMed in the form of monies or fees paid for services from EyeMed. EyeMed had knowledge of this benefit when it accepted the money from Plaintiff and the class members.

123. The monies or fees paid by the Plaintiff and class members were supposed to be used by EyeMed, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and class members.

124. EyeMed failed to provide reasonable security, safeguards, and protections to the personal data of Plaintiff and class members, and as a result the Plaintiff and class overpaid EyeMed as part of services they purchased.

125. EyeMed failed to disclose to Plaintiff and members of the class that its computer systems and security practices were inadequate to safeguard users' and former users' personal data against theft.

126. Under principles of equity and good conscience, EyeMed should not be permitted to retain the money belonging to Plaintiff and class members because EyeMed failed to provide adequate safeguards and security measures to protect Plaintiff's and class members' personal, health, and financial information that they paid for but did not receive.

127. EyeMed wrongfully accepted and retained these benefits to the detriment of Plaintiff and class members.

128. EyeMed's enrichment at the expense of Plaintiff and class members is and was unjust.

129. As a result of EyeMed's wrongful conduct, as alleged above, Plaintiff and the class are entitled under the unjust enrichment laws of all 50 states and the District of Columbia to restitution and disgorgement of all profits, benefits, and other compensation obtained by EyeMed, plus attorneys' fees, costs, and interest thereon.

RELIEF REQUESTED

Plaintiff, individually and on behalf of the proposed class, requests that the Court:

1. Certify this case as a class action on behalf of the class defined above, appoint Plaintiff as class representative, and appoint the undersigned counsel as class counsel;

2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other class members;

3. Award restitution and damages to Plaintiff and class members in an amount to be determined at trial;

4. Award Plaintiff and class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

5. Award Plaintiff and class members pre- and post-judgment interest, to the extent allowable; and

6. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

/s/ Terence R. Coates
W.B. Markovits (0018514)
Terence R. Coates (0085579)

Zachary C. Schaengold (0090953)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
bmarkovits@msdlegal.com
tcoates@msdlegal.com
zschaengold@msdlegal.com
dgould@msdlegal.com

Lori G. Feldman (*pro hac vice forthcoming*)
GEORGE GESTEN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton- On-Hudson, NY 10502
Phone: (917) 983-9321
Fax: (888) 421-4173
LFeldman@4-Justice.com

David J. George *(pro hac vice forthcoming)*
Brittany L. Brown (*pro hac vice forthcoming*)
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite 302
Lake Worth, FL 33463
Phone: (561) 232-6002
Fax: (888) 421-4173
DGeorge@4-Justice.com
BBrown@4-Justice.com

Bryan L. Bleichner (*pro hac vice forthcoming)*
Jeffrey D. Bores (*pro hac vice forthcoming)*
Christopher P. Renz (*pro hac vice forthcoming)*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
crenz@chestnutcambronne.com

Counsel for Plaintiff and the Class